Before the

FEDERAL COMMUNICATIONS COMMISSION

Washington, D.C.

In the Matter of	)	
Establishment of Technical Requirements and Standards for Telecommunications Carrier Assistance Capabilities Under the Communications Assistance for Law Enforcement Act	)	CC Docket No. 97-213

COMMENTS IN OPPOSITION TO THE FBI'S AND DOJ'S JOINT PETITION FOR EXPEDITED RULEMAKING

Americans for Tax Reform
1320 18th Street, NW
Suite 200
Washington, D.C. 20036
(202) 785-0266

Center for Technology Policy
Free Congress Foundation
717 Second Street, NE
Washington, D.C. 20002
(202) 546-3000

Citizens for a Sound Economy
1250 H Street, NW
Suite 700
Washington DC 20005
(202) 783-3870

May 20, 1998

TABLE OF CONTENTS

SUMMARY

With these comments, Americans for Tax Reform, the Center for Technology Policy of the Free Congress Foundation, and the Citizens for a Sound Economy hereby oppose the Joint Petition for Expedited Rulemaking filed by the Federal Bureau of Investigation and the Department of Justice. The Joint Petitioners have requested that the Federal Communications Commission improperly enforce the Communications Assistance for Law Enforcement Act (CALEA) by expanding law enforcement electronic surveillance capabilities, contrary to the intent of CALEA.

The government is seeking the adoption of rules that would require the telecommunications system to be designed as a surveillance device -- a purpose that goes far beyond the intent of CALEA. The federal law enforcement agencies are not trying to just maintain the status quo, but are seeking rules that will result in the delivery of call content and call-identifying information that law enforcement has not previously received, nor that has been mandated by CALEA.

CALEA was not designed to expand the ability of law enforcement agencies to conduct electronic surveillance; rather it was enacted as part of a narrowly circumscribed effort to respond to developments in communications technology that, in some respects, had made electronic surveillance of communications by law enforcement officials more difficult than such activity had been in the past. Congress made clear in enacting CALEA that the purpose of the

legislation was simply to "preserve" the government's existing surveillance capabilities, not to expand them.

CALEA was an attempt to maintain a balance between privacy interests and law enforcement in the midst of continuing developments in law and communications technology. In the Joint Petition, the FBI and the Department of Justice misrepresent the intent and language of CALEA, as well as the repeated statements by FBI Director Louis Freeh, and request an impermissible intrusion into individuals' privacy with their petition for expedited rulemaking. This attempt to use the expanded technological capabilities of communications networks to create expanded surveillance capabilities over American citizens is flatly contrary to federal law governing wiretapping, and to the privacy protections established by the Fourth Amendment to the United States Constitution.

Before the

FEDERAL COMMUNICATIONS COMMISSION

Washington, D.C.

In the Matter of	)	
Establishment of Technical Requirements and Standards for Telecommunications Carrier Assistance Capabilities Under the Communications Assistance for Law Enforcement Act	)	CC Docket No. 97-213

To: The Commission

COMMENTS OF AMERICANS FOR TAX REFORM, THE CENTER FOR TECHNOLOGY POLICY OF THE FREE CONGRESS FOUNDATION, AND CITIZENS FOR A SOUND ECONOMY

In response to the Commission's Public Notice in the above-captioned proceeding, DA 98-762 (released April 20, 1998), and pursuant to Section 1.405 of the Commission's rules, 47 C.F.R. § 1.405 (1997), Americans for Tax Reform, The Center For Technology Policy of the Free Congress Foundation, and Citizens For a Sound Economy hereby oppose the Joint Petition for Expedited Rulemaking filed by the Federal Bureau of Investigation ("FBI") and the Department of Justice ("DOJ"). Section 107(b) of the Communications Assistance for Law Enforcement Act ("CALEA") establishes a standards-setting role for the Federal Communications

Commission. 47 U.S.C. § 1006(b). However, commenters oppose the efforts of the FBI and DOJ to use the process of Section 107(b) to improperly expand their electronic surveillance capabilities, contrary to the intent of the law.

Americans for Tax Reform ("ATR") serves as a national clearinghouse for the grassroots taxpayers' movement by working with approximately 800 state and county-level groups. ATR opposes all tax increases as a matter of principle, wanting to minimize the government's power to control individuals' lives. Further, ATR is opposed in general to government intrusion into individuals' lives and privacy. As digital commerce becomes an increasingly important part of the economy, ATR is particularly concerned that all future tax and regulatory systems be designed in such a way as to maximize the privacy and security of all taxpayers and citizens doing business on the Internet, or using network-enabled communications devices to do business, whether by means of wired or wireless communications systems.

Citizens for a Sound Economy ("CSE") wants to promote a competitive and deregulated economy in all facets of the market, including the telecommunications industry. CSE believes that consumers can benefit most from increased competition and choice in communications, rather than regulation and monopoly. The government should not restrict or mandate technological development, nor should the government compromise the privacy rights of individuals.

The Center for Technology Policy of the Free Congress Research and Education Foundation focuses on technology topics such as encryption, medical privacy, biometric technology, government surveillance and national databases for the Free Congress Foundation. The Free Congress Foundation was founded in 1977 as a non-partisan, non-profit research and education institute dedicated to conservative governance, traditional values and institutional reforms.

I. The Potential Expansion of Electronic Surveillance Capabilities Presents a Significant Threat to the Future of Individual Privacy

This proceeding will have significant ramifications for the future of privacy in the United States. The government is seeking the adoption of rules that would require the telecommunications system to be designed as a surveillance device -- a purpose that goes far beyond the intent of CALEA. As the Joint Petition points out, the government is seeking rules to facilitate electronic surveillance "at a centralized point" that is "accomplished through the use of software employed by the carrier to route authorized information to law enforcement officers." Jt. Pet. at 10-11. Accordingly, the federal law enforcement agencies are not trying to just maintain the status quo, but are seeking rules that "will result in the delivery of call content and call-identifying information that law enforcement has not previously received." Id. at 26. The Joint Petition states plainly that "Section 103 does not restrict this obligation to those communications and call-identifying information that were accessible to law enforcement in the pre-digital era." Specifically, it seeks rules mandating access to "new information [that] is generated" from "the evolution of services and technologies." Id.

This naked attempt to leverage the expanded technological capabilities of communications networks to create expanded surveillance capabilities over American citizens is flatly contrary to federal law governing wiretapping. The dissonance is revealed, in part, by the government's scant discussion of the Electronic Communications Privacy Act of 1986 (18 U.S.C. § 2510 et seq.) ("ECPA"), which it describes as nothing more than an "update" of Title III provisions to "clarify federal privacy protections and electronic surveillance standards in light of changes in computer and telecommunications technologies." Id. at 6. Far from this tepid description of the 1986 law, ECPA represented a substantive change in federal law to expand privacy protections enacted to prevent their erosion by advancing digital technology.

ECPA was premised on the recognition that the law had not kept pace with the development of new electronic technologies, and that "the use of sophisticated technologies for surveillance purposes . . . presents dangers to society." Office of Technology Assessment, ELECTRONIC SURVEILLANCE AND CIVIL LIBERTIES 11 (OTA-CIT-293, October 1985). The Congressional Office of Technology Assessment found that the use of advanced technology for surveillance could infringe upon First, Fourth and Fifth Amendment protections, as well as the statutory safeguards of Title III and other laws. Id. at 11-12. It concluded that "[o]ver time, the cumulative effect of widespread surveillance for law enforcement, intelligence, and other investigatory purposes could change the climate and fabric of society in fundamental ways." Id. at 11.

Such findings were foremost in the minds of ECPA's architects. As the Senate Report on ECPA noted, "[w]hen the Framers of the Constitution acted to guard against the arbitrary use of government power to maintain surveillance over citizens, there were limited methods of intrusion into the 'houses, papers, and effects' protected by the fourth amendment." S. Rep. 99-541, 99th Cong., 2d Sess. 1-2 (Oct. 17, 1986). It added that "development of new methods of communication and devices for surveillance has expanded dramatically the opportunities for such intrusions." Id. at 2. After pointing to "tremendous advances in telecommunications and computer technologies" as well as surveillance techniques, the Report stated that "[e]lectronic hardware making it possible for overzealous law enforcement agencies, industrial spies and private parties to intercept the personal or proprietary communications of others" required changes in Title III. Id. at 3. It concluded that "the law must advance with the technology to ensure the continued vitality of the fourth amendment. Privacy cannot be left to depend solely on physical protection, or it will gradually erode as technology advances. Congress must act to protect the privacy of our citizens. If we do not, we will promote the gradual erosion of this precious right." Id. at 5.

Congress did not make this change out of devotion to some abstract principle. Rather it was well aware of a history of "tapping and bugging [in which the government] targeted many people who might not normally appear to be appropriate targets." See ELECTRONIC SURVEILLANCE AND CIVIL LIBERTIES, supra at 32. Indeed, the Church Committee investigations in the 1970s revealed the FBI

had used electronic surveillance to investigate Dr. Martin Luther King, Jr., Congressman Harold Cooley, dissident groups and journalists among many others. 1/ After providing detailed accounts of improper use of electronic surveillance by the FBI and other government agencies, the Church Committee noted that "[t]echnological developments in this century have rendered most private conversations of American citizens vulnerable to interception and monitoring by government agents." Church Committee Report, Vol. III at 273.

Accordingly, the Report found:

> By their very nature . . . electronic surveillance techniques also provide the means by which the Government can collect vast amounts of information, unrelated to any legitimate governmental interest, about large numbers of American citizens. Because electronic monitoring is surreptitious, it allows Government agents to eavesdrop on the conversations of individuals in unguarded moments, when they believe they are speaking in confidence. Once in operation, electronic surveillance techniques record not merely conversations about criminal, treasonable, or espionage-related activities, but all conversations about the full range of human events. Neither the most mundane nor the most personal nor the most political expressions of the speakers are immune from interception. Nor are these techniques sufficiently precise to limit the conversations overheard to those of the intended subject of the surveillance: anyone who speaks in a bugged room and anyone who talks over a tapped telephone is also overheard and recorded.

1/ ELECTRONIC SURVEILLANCE AND CIVIL LIBERTIES, supra, at 32. See Senate Select Committee to Study Governmental Operations With Respect to Intelligence Activities, 94th Cong., 2d Sess. (1976) ("Church Committee Report").

> The very intrusiveness of these techniques implies the need for strict controls on their use, and the Fourth Amendment protection against unreasonable searches and seizures demands no less. Without such controls, they may be directed against entirely innocent American citizens, and the Government may use the vast range of information exposed by electronic means for partisan political and other improper purposes. Yet in the past the controls on these techniques have not been effective; improper targets have been selected and politically useful information obtained through electronic surveillance has been provided to senior administration officials.

Id. at 274. Lest the Commission make the mistake of assuming that such abuses were limited to a particular era, it should examine recent reports suggesting that major police departments have evaded legal controls on wiretapping, and have ignored requirements governing its use. It has been estimated that in Los Angeles alone there have been "hundreds of secret 'handoff' taps and electronic intercepts, [and] by extrapolation, thousands of Los Angeles residents have had their telephone conversations secretly and illegally monitored by LAPD." 2/ Accordingly, it should come as no surprise that the vast majority of Americans disapprove of wiretapping as an investigative tool. 3/

2/ See, e.g., Charles L. Lindner, Can the L.A. Criminal Justice System Work Without Trust?, LA Times (April 26, 1998) (describing fraudulent methods by which police obtain warrants and revealing that for the past thirteen years law enforcement authorities in Los Angeles have ignored the legal requirement to keep an inventory of tapped conversations as a prerequisite to continuing authorization).

3/ During fifteen years of surveys conducted by the Department of Justice, the percentage of the U.S. population that approved of the use of wiretapping never exceeded 30 percent. The level of disapproval ranged from 70 to 80 percent across all demographic groups. Bureau of Justice Statistics, Sourcebook of Criminal Justice Statistics -- 1992.

In light of this background, it is not possible that Congress intended through CALEA to expand the FBI's electronic surveillance capabilities to enable the government to take advantage of the possibilities offered by advancing technology, as the government now contends. Quite to the contrary, Congress meant for the law to be read "narrowly" as detailed below.

II. CALEA Was Not Designed to Expand the Ability of Law Enforcement Agencies to Conduct Electronic Surveillance

Congress enacted "CALEA" as part of a narrowly circumscribed effort to respond to developments in communications technology that, in some respects, had made electronic surveillance of communications by law enforcement officials more difficult than such activity had been in the past.4/ Congress made clear in enacting CALEA that the purpose of the legislation was simply to "preserve" the government's existing surveillance capabilities,5/ not to expand them.6/ Thus,

---

4/ H.R. Rep. No. 827, 103d Cong., 2d Sess., pt. 1, at 3492, 3493 (1994), reprinted in 1995 U.S.C.C.A.N. 3489, 3496 ("House Report"). See also Cellular Telecommunications Industry Association ("CTIA") , et al., Digital Issues Interim Report: Communications Privacy in the Digital Age 23 (1997) ("Communications Privacy in the Digital Age").

5/ House Report at 3489, 3492, 3497, 3498, 3502.

6/ Id. at 3497 ("The bill will not expand [the] authority" of law enforcement agencies to conduct wiretaps pursuant to court order. "[A]s the potential intrusiveness of technology increases, it is necessary to ensure that government surveillance authority is clearly defined and appropriately limited."), 3498, 3502, 3503; see also 47 U.S.C. §§ 1002(a)(4), 1002(b); Digital Telephony and Law Enforcement Access to Advanced Telecommunications Technologies and Services: Hearings before the Subcommittee on Technology and the Law, Senate Judiciary Committee, and the Subcommittee on Civil and Constitutional Rights, S. Hrg. No. 1022, 103rd Cong., 2d Sess. 29 (1994) (testimony of Louis J. Freeh, Director, Federal Bureau of Investigation) ("Senate Hearing").

according to Congress, "the bill seeks to balance three key policies: (1) to preserve a narrowly focused capability for law enforcement agencies to carry out properly authorized intercepts; (2) to protect privacy in the face of increasingly powerful and personally revealing technologies; and (3) to avoid impeding the development of new communications services and technologies."7/

A. Statutory Background of CALEA

CALEA is the latest in a series of congressional efforts to establish and maintain a balance between the interests of privacy and law enforcement in the midst of continuing developments in law and communications technology.8/ Congress' first effort to achieve this balance was its enactment in 1968 of the Omnibus Crime Control and Safe Streets Act ("1968 Act").9/ The 1968 Act prohibited the use of electronic surveillance by private individuals. At the same time, however, the Act created a judicial process by which law enforcement officials could obtain a court's authorization to conduct such surveillance.10/ The legislation was a response, in part, to advances in communications technology which Congress felt posed a threat to individual privacy. The legislation was also a response, however, to the Supreme Court's 1967 holding that electronic surveillance

---

7/ House Report at 13.

8/ See House Report at 3491-93.

9/ NPRM at ¶ 2; House Report at 3491.

10/ NPRM at ¶ 2; citing House Report at 3491.

constituted a search and seizure within the meaning of the Fourth Amendment.11/ The 1968 Act's "dual purpose" was to "(1) protect[] the privacy of wire and oral communications and (2) delineat[e] on a uniform basis the circumstances and conditions under which the interception of wire and oral communications may be authorized."12/

In the years since 1968, Congress has engaged in what has become a continual rebalancing process. In 1970, the United States Court of Appeals for the Ninth Circuit held that the 1968 Act neither required carriers to provide the technical support needed by law enforcement to conduct authorized electronic surveillance, nor authorized the courts to compel such support.13/ Congress responded that same year by amending the 1968 Act to provide that any order issued by a federal court authorizing an electronic interception must, upon request of the government, direct communications service providers to provide all information, facilities, and technical assistance necessary to accomplish the interception.14/

11/ Katz v. United States, 389 U.S. 347, 353 (1967).

12/ House Report at 3491, quoting Senate Committee on the Judiciary, Omnibus Crime Control and Safe Streets Act of 1967, S. Rep. No. 1097, 90th Cong., 2d Sess. 66 (1968).

13/ Application of the United States for Relief, 427 F.2d 639, 643-44 (9th Cir. 1970); see also NPRM at ¶ 3.

14/ 18 U.S.C. § 2518(4); NPRM at ¶ 3.

As noted above, continuing technological developments again prompted Congress to take legislative action in 1986 through passage of ECPA.15/ The law extended both the privacy protections and the surveillance authority established in the 1968 Act to emerging services and technologies, such as electronic mail, cellular telephones, and paging devices.16/ The purpose of this legislation was again to maintain a balance between the privacy of citizens and the needs of law enforcement.17/

CALEA represents Congress' most recent effort to "preserve the balance sought in 1968 and 1986" in the face of a now accelerated pace of change in telecommunications technology.18/ Although the legislation enacted in 1968 and 1970 had made clear that telecommunications carriers were required to cooperate with law enforcement personnel in conducting electronic surveillance, CALEA is the first statute to impose upon carriers an affirmative obligation to modify and design

---

15/ Electronics Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1872 (1986). "Electronic communication" is defined in that Act as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire. radio, electromagnetic, photoelectric or photooptical system that affects interstate or foreign commerce, but does not include - (A) any wire or oral communication; (B) any communication made through a tone-only paging device; (C) any communication from a tracking device (as defined in section 3117 of [Title 18])." Id.

16/ House Report at 3491-92; see also NPRM at ¶ 3.

17/ House Report at 3492, citing and quoting House Committee on the Judiciary, Electronic Communications Privacy Act of 1986, H.R. No. 99-647, 99th Cong., 2d Sess., pt. 2, at 19 (1986).

18/ House Report at 3492.

their equipment, facilities, and services "to ensure that new technologies and services do not hinder law enforcement's access to the communications of a subscriber who is the subject of a court order authorizing electronic surveillance."19/ However, in enacting CALEA, Congress also made clear that the statute was intended only to preserve the status quo in surveillance capabilities. According to Congress, CALEA was intended to set "both a floor and a ceiling" on the ability of law enforcement to conduct electronic surveillance.20/ In other words, therefore, while the statute was intended to ensure that new technologies would not reduce law enforcement's existing surveillance capabilities, it also was carefully crafted to prevent any expansion of those capabilities.21/

B. CALEA Requirements

Section 103(a) of CALEA establishes four general capability requirements that carriers will be required to meet by October 25, 1998. 22/ Under Section 103(a), carriers must be capable of:

> (1) expeditiously isolating, and enabling the government to intercept, all wire and electronic communications within that carrier's network to, or from, a specific subscriber of such carrier;
>
> (2) expeditiously isolating, and enabling the government to access, call-identifying information that is reasonably available to the carrier;

19/ Id. at 3496; NPRM at ¶¶ 1,6.

20/ Id. at 3502.

21/ See id. at 3497, 3502.

22/ 47 U.S.C. § 1002(a), § 1001 note.

(3) delivering intercepted communications and call-identifying information to a location specified by the government, other than the premises of the carrier; and

(4) conducting interceptions and providing access to call-identifying information unobtrusively.23/

CALEA also, however, "expands privacy and security protection for telephone and computer communications."24/ For example, Section 103(a)(4)(A) affirmatively requires carriers to perform their obligations under the statute "in a manner that protects -- [] the privacy and security of communications and call-identifying information not authorized to be intercepted" by law enforcement.25/ Section 103(a)(2) explicitly prohibits the use by law enforcement of pen registers and trap and trace devices to obtain tracking or location information on a targeted subscriber, other than that which can be determined from a telephone number.26/ Section 208 requires that law enforcement use reasonably available technology to minimize information obtained through pen registers.27/ Section 207 enhances the protection of electronic mail ("e-mail") and other transactional data, such as transactional logs containing a person's entire on-line profile, by requiring the

---

23/ Id. § 1002(a); In the Matter of Communications for Law Enforcement Act, Notice of Proposed Rulemaking, CC Docket No. 97-213, FCC 97-356 (rel. October 10, 1997), at ¶ 40 ("NPRM").

24/ House Report at 3490.

25/ 47 U.S.C. § 103(a)(4)(A).

26/ Id. § 103(a)(2); House Report at 3498.

27/ 18 U.S.C § 2516(1); House Report at 3497.

presentation of a court order by law enforcement officials, rather than a mere administrative subpoena, to obtain such information.28/

The statute also:

- requires affirmative intervention of a common carrier's personnel for switch-based interceptions, so that law enforcement will not be able to activate interceptions remotely or independently within the switching premises of a carrier;29/
- extends existing statutory privacy protections to cordless telephones and certain data communications transmitted by radio;30/
- protects the rights of subscribers to encrypt communications;31/
- allows any person, including public interest groups, to petition the FCC for review of standards implementing wiretap capability requirements, and provides that one factor for judging those standards is whether they protect the privacy of communications not authorized to be intercepted;32/
- does not require mobile service providers to reconfigure their networks to deliver the content of communications occurring outside a carrier's service area;33/ and
- improves the privacy of mobile phones by expanding criminal penalties for using certain devices to steal mobile telephone service.34/

28/ 18 U.S.C. § 2703; House Report at 3490; NPRM at ¶ 7.

29/ House Report at 3497-98

30/ 18 U.S.C. § 2511(4); House Report at 3490; NPRM at ¶ 7.

31/ 47 U.S.C. § 1002(b)(3).

32/ Id. § 1006(b).

33/ Id. § 1002(d).

34/ 18 U.S.C. §§ 1029(a), 1029(c)(2).

C. Law Enforcement Agencies Pledged Not to Seek an Increased Ability to Conduct Surveillance

During Congress' deliberations on CALEA, the FBI emphasized that CALEA was not intended to expand law enforcement surveillance capabilities. FBI Director Louis J. Freeh testified before Congress that CALEA was intended only to maintain the ability of law enforcement to conduct electronic surveillance, not to "expand the current laws authorizing the interception of wire or electronic communications."35/ As quoted in the House Report on CALEA, Director Freeh testified that CALEA

> was intended to preserve the status quo, that it was intended to provide law enforcement no more and no less access to information than it had in the past.36/

Furthermore, the House Report states that Director Freeh "supported in his testimony" several of the provisions in CALEA that expanded privacy protections for telephone and computer communications.37/

The House Report's repeated references to Director Freeh's testimony and lengthy discussions concerning the manner in which CALEA would protect privacy demonstrate that in enacting CALEA,38/ Congress relied heavily on the FBI's assurances that law enforcement did not intend to use the legislation as a vehicle

---

35/ Senate Hearing at 29.

36/ House Report at 3502.

37/ Id. at 3497.

38/ See id. at 3497-3500, 3503-04.

through which to increase the government's electronic surveillance capabilities. Indeed, it was out of concern that law enforcement would so abuse CALEA that Congress included in the legislation not only prescriptive measures to protect individual privacy, but also affirmative obligations on the part of carriers to protect such privacy.39/

III. The FBI and Justice Department Are Trying to Use the FCC Proceeding to Thwart CALEA Mandates

A. The Joint Petition is Seeking FCC Ratification of Expanded Electronic Surveillance Capabilities

As is now clear from the government's Joint Petition, the FBI and Justice Department are seeking to use the FCC's rulemaking process to expand their wiretapping capabilities beyond what Congress authorized in adopting CALEA. Directly contravening both congressional intent and previous representations, the FBI and other law enforcement agencies have demanded broad, new surveillance capabilities which far exceed the capabilities set forth, and explicitly established as a ceiling, in Section 103(a) of the Act.40/ As described

---

39/ It was also out of this concern that Congress included in the House Report the statement that in enacting standards to allow implementation of CALEA's requirements, Congress "expect[ed] industry, law enforcement and the FCC to narrowly interpret the requirements" set forth in Section 103 of the Act. Id. at 3502-03.

40/ See 47 U.S.C. § 1002(a); House Report at 3502. Section 103(b)(1) of CALEA directs that industry associations and standard-setting organizations should bear primarily responsibility for the development of technical standards to implement the law. 47 U.S.C. § 1002(b)(1); Id. at 3499, 3503. According to Congress, "law enforcement agencies are not permitted to require the specific design of systems or features, nor prohibit adoption of any such design, by wire or electronic communications providers or equipment manufacturers." Id. at 3503. Nevertheless, the FBI and other law enforcement agencies have twice blocked the adoption of

below, the increased eavesdropping capabilities sought by the FBI would likely violate not only the specific provisions of CALEA, but also the constitutional privacy protections established by the Fourth Amendment's search and seizure clause. Among the expanded capabilities demanded are the following:

Location Information on Wireless Calls: Through CALEA, the FBI seeks the ability to obtain information on the location of wireless customers as customers roam between cell sites. However, Section 103(a)(2) denies law enforcement such capabilities by stating that carriers may only enable the government to access call-identifying information

> (A) before, during, or immediately after the transmission of a wire or electronic communication (or at such later time as may be acceptable to the government); and (B) in a manner that allows it to be associated with the communications to which it pertains, except that, with regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices (. . .), such call-identifying information shall not include any information that may disclose the physical location of the subscriber (except to the extent that the location may be determined from the telephone number)."41/

Moreover, FBI Director Freeh testified prior to enactment of CALEA that the "call-identifying information" that could be obtained without a warrant under CALEA

> does not include any information which might disclose the general location of a mobile facility or service, beyond that associated with the area code or exchange of the facility or service. There is no intent

---

standards proposals reflecting hard-won industry consensus because the proposals failed to include all of the expanded capabilities that these agencies have demanded.

41/ 47 U.S.C. § 1002(a)(2).

whatsoever, with reference to this term, to acquire anything that could properly be called "tracking" information.42/

Monitoring of Multi-Party Conference Calls: The FBI also seeks the ability to continue monitoring all parties to a multi-party conference call even after the legally designated subject of an intercept order -- the subject of investigation -- has dropped off the call. In addition, the FBI seeks the ability to obtain information on the identities of all parties to a conference call as they join or leave it, whether or not the subject is, or ever was, on the line. These capabilities are specifically denied by Section 103(a)(4) of CALEA, which expressly directs carriers to perform their obligations under the statute "in a manner that protects . . . the privacy and security of communications and call-identifying information not authorized to be intercepted."43/

Access to Content Information Without a Warrant: Currently, law enforcement can obtain information on the dialing and signaling information utilized in processing a call that a subject of investigation has placed (the "electronic or other impulses which identify the numbers dialed or otherwise transmitted"44/) using a "pen register" issued, without a warrant, by an Assistant United States Attorney. The FBI seeks to expand the information it can obtain under a pen register order to include the complete content of any information

---

42/ Senate Hearing at 6 (testimony of Louis J. Freeh, Director, Federal Bureau of Investigation).

43/ 47 U.S.C. § 1002(a)(4).

44/ 18 U.S.C. § 3127(3).

transmitted via packet switching technologies. Again, however, this capability would violate the Section 103(a)(4) requirement that carriers must "protect [] the privacy and security of communications and call-identifying data not authorized to be intercepted."45/

Access, Without a Warrant, to Digits Dialed After a Call is Connected: The FBI also seeks to expand the information it can obtain under a pen register order to include information on the digits a subject dials after a call is connected (e.g., to access an information service). However, because Congress wanted to maintain the distinction between call-identifying data and call content, Congress included in CALEA a requirement that law enforcement, when executing pen registers, must use equipment "that restricts the recording or decoding of information utilized in call processing."46/ In addition, the House Report on CALEA states that "[o]ther dialing tones that may be generated by the sender that are used to signal customer premises equipment of the recipient are not to be treated as call identifying information."47/

Notification, Without a Warrant, of When the Subject is Signaled by Network Messages: The FBI also seeks the authority to obtain, under pen register orders, notification of when a subject is signaled by network services, such as call-waiting flashes and voice mail message waiting indicators. This information cannot

---

45/ 47 U.S.C. § 1002(a)(4)(A).

46/ 18 U.S.C. § 3121(c).

47/ House Report at 3501.

be considered "call-identifying information," and thus falls outside the information obtainable under the statute.

Access, Without a Warrant, to Other Enhanced Services and Features: Also pursuant to pen register orders, the FBI seeks to obtain access to other enhanced services utilized by a subject, such as party hold, drop, and join messages, as well as flash hooks and other feature key usage. As before, however, this information cannot be considered "call-identifying information," and thus exceeds the scope of information obtainable under the statute.

Notification of Changes in a Subject's Customer Service Profile: The FBI seeks a requirement that carriers must send a message to law enforcement on the subject's line whenever the subject's services are altered in response to a request by the subject. This would, in effect, constitute a requirement that carriers generate a type of on-line customer service profile for use by law enforcement personnel. Such information currently is provided only by subpoena and should continue to be subject to this important restriction.

B. The Government's Proposed Standards Are Contrary to the Law

In advocating the "broad" interpretation of CALEA (Jt. Pet. ¶59), the FBI contradicts not only the express intent of the House Judiciary Committee, but also the repeated statements by its Director, Louis Freeh. Concerned that law enforcement might try to capitalize on technological innovations to erode Fourth Amendment rights, Congress specifically drafted narrow legislation, and repeatedly urged against any overbroad interpretation of the requirements of CALEA. H.Rep.

103-827 at 16, 22, 23 and 27. "The Committee expects industry, law enforcement and the FCC to narrowly interpret the requirements [of CALEA]." Id. at 23.

Director Freeh appeared to echo these desires for narrow interpretations, claiming that the FBI needed CALEA only to avoid the de facto repeal of existing statutory authority. "[CALEA] explicitly states that the legislation does not enlarge or reduce the government's authority to lawfully conduct court-ordered electronic surveillance." Senate Hearings at 16 (March 18, 1994 statement of FBI Director Louis Freeh). However, the breadth of access that the Joint Petition advocates for law enforcement greatly surpasses Freeh's statements, and congressional intent.

We urge the FCC to not follow the incorrect standards set forth in the Joint Petition, rather to heed the Congress in narrowly interpreting the CALEA requirements by rejecting the Joint Petition. Congress intended to preserve the privacy of non-targeted communications while maintaining law enforcement's current level of surveillance capabilities. H.Rep. 102-827 at 27. "The FCC is directed to protect privacy and security of communications that are not targets of court-ordered surveillance and to serve the policy of the United States to encourage the provision of new technologies and services to the public." Id.

The FBI is attempting to use technological innovations in telecommunications to gather unconstitutionally intrusive information from targets, but CALEA clearly was not intended "to guarantee 'one stop shopping' for law enforcement." Id. at 22. As the ability and intrusiveness of technology